2-party 及 3-party 匿名式認證金鑰

簡宏宇
國立暨南國際大學資訊管理所
hychien@ncnu.edu.tw

廖文立
國立暨南國際大學資訊管理所
s97213528@ncnu.edu.tw

***摘要*—近年來，以密碼(password)為基礎的認證機制-由於有著能讓使用者自己選擇簡單好記的密碼，且不需要其他的輔助設備的優點-被廣泛的用於使用者的認證上。過去的以密碼基礎的認證金鑰協定多忽略匿名性需求，然而在有些應用中卻需要保護使用者的身份。這篇文章提出一個支援匿名(anonymous)的 2-Party Anonymous Encrypted Key Exchange (2P-AEKE) 及一個匿名 3-Party Anonymous Encrypted Key Exchange (3P-AEKE) 機制以滿足此需求。**

***關鍵詞*—認證、3PEKE、匿名。**

一、 簡介

早在 1976 年，Diffie 和 Hellman[10]兩位學者就提出了一套非對稱的金鑰交換協定。但是 Diffie-Hellman 的機制很容易受到中間人攻擊(man-in-middle attack)，因為在此機制中，通訊的雙方缺少了驗證彼此是否合法的機制。因此，後續有很多學者(如 1999 年，Seo 和 Sweeney[2]提出了一個名為 SAKA 的金鑰交換機制)提出認證式金鑰協定以解決此問題。

在 2000 年，Tseng[11]指出 SAKA 無法抵擋重送攻擊(replay attack)，並提出一個機制來改善。同樣在 2000 年，Ku 和 Wang[9]指出 Tseng 的機制會受到偽造攻擊(modification attack)，並提出一個機制來改善。不幸的，在 2003 年，Hsu 等人[1]指出 Ku 和 Wang 的機制仍會遭受偽造攻擊。2004 年 Lee 和 Lee[7]兩位學者指出 Hsu 的機制仍然可能受到偽造攻擊，並提出了一個方法來改善這個機制。在 2005 年，另外兩位學者 Lee 和 Lee[6]指出 Lee-Lee 的機制會受到中間人攻擊，提出新的方法來增強這個機制。在 2008 年，Yoon 和 Yoo[3]指出，Lee-Lee 的機制可能會遭受到離線式的密碼猜測攻擊(off-line password guessing attack)，並提出一個機制來改善這個問題。

而一個以密碼為基礎的 3PEKE(Three Party Encrypted Key Exchange protocol)，他透過一個可供信任的第三方，讓兩個使用者可以建立屬於他們的會議金鑰(session key)，而這些使用者只需與此可信任的第三方儲存一組密碼；此方式在分散式環境下具有較佳的擴充性。然而，如何在提高密碼的強度和使用者的便利性間取得平衡就成了此類機制重要的議題。典型以密碼為基礎的 3PEKE 有 Lu-Cao[8]和 Chung-Ku[4]提出的 3PEKE，但是他們都忽略了一項可能的威脅，那就是離線式的密碼猜測攻擊。在 2008 年，Chien[5]提出了一種將密碼經過處理，轉換成驗證碼的機制，來防止離線式的密碼猜測攻擊。另外，之前的研究也都先忽略匿名需求。

本篇文章分成以下幾個段落：第二段介紹我們提出的匿名認證金鑰協定，分為 2-party 和 3-party 兩部分；第三段進行效能及安全性的分析，第四段做個結論。

二、所提出的匿名認證金鑰協定

第一節先介紹由兩個通訊雙方就可以完成的匿名機制，第二節介紹經由一個可以信任的第三方所完成的匿名機制。

2.1 Two-Party Anonymous Encrypted Key Exchange

此機制所設定的情境是主從式通訊架構：通訊的客戶端 (client)已知其伺服器(server)的名稱或連結方式- 可能是其 IP address 或在無線通訊時確知伺服器在其訊號範圍，且想以匿名方式建立金鑰以保護其真實身份不被第三者知道。

圖 3.1 是我們所提出的 Two-Party Anonymous Encrypted Key Exchange(2-PAEKE)的資料傳遞過程，下面情境假設 A 是客戶端，B 是伺服器端：

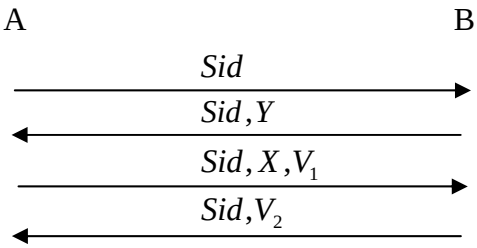

圖 3.1 2P-AEKE

步驟一. A→B：Sid

A 先對 B 送出建立通訊的請求。

步驟二. B→A：Sid,Y

B 收到 A 的請求後，隨機選擇一個亂數 b，計算出 $Y=g^b$ 後，將值傳回。

步驟三. A→B：Sid,X,V_1

A 收到 B 傳回的資料，隨機選擇一個亂數 a，算出 $X=g^a$ 和

$V_1=E_{g^{ab}}(ID_A,Y,M_1=g^a\oplus g^{pw})$，將 Sid,X,V_1 傳回。

步驟四. B→A：Sid,V_2

B 收到 A 的資料，先解出 V_1 裡的資料，取得 ID_A 後，找出相對應的密碼 pw，計算 $M_1\oplus g^{pw}$ 的值是否等於 X，如果是，則計算 $V_2=E_{g^{ab}}(ID_A,ID_B,M_2=g^b\oplus g^{pw})$，將 Sid,V_2 傳回。

A 收到資料後將 V_2 的值解開，計算 $M_2\oplus g^{pw}$ 是否等於收到的 Y。

2.2 Three-Party Anonymous Encrypted Key Exchange

相較於 2-party 協定，3-party 協定因有信賴的第三者協助，每位使用者只需記住一組密碼或金鑰，因而它具有較佳的擴充性。下圖 3.2 是我們所提出的 Three-Party Anonymous Encrypted Key Exchange(3P-AEKP)的資料傳遞過程：

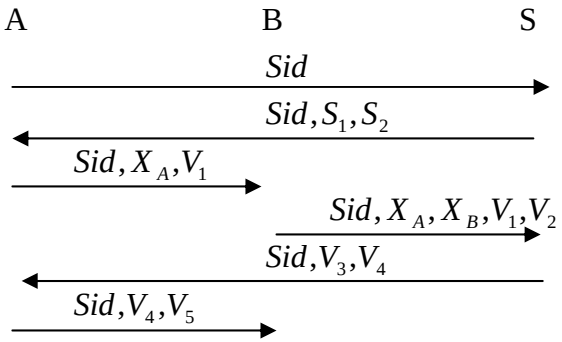

圖 3.2 3P-AEKE

步驟一. A→S：Sid

A 先向 Server 端發出通訊的要求。

步驟二. S→A：Sid,S_1,S_2

S 在收到 A 所提出的要求後，隨機選擇兩個亂數 z_1,z_2，計算 $S_1=g^{z_1},S_2=g^{z_2}$，並將值傳出。

步驟三. A→B：Sid,X_A,V_1

A 收到 S 傳回的資料後，隨機選擇一個亂數 a，計算出 $X_A=g^a$ 和

$V_1 = E_{g^{az_1}}(ID_A, g^{a \cdot pw_A})$ 後傳出。

步驟四，B→S：Sid, X_A, X_B, V_1, V_2

在收到資料後，B 隨機選擇一個亂數 b，計算出 $X_B = g^b$ 和 $V_2 = E_{g^{bz_2}}(ID_B, g^{b \cdot pw_B}, g^{ab})$，並將計算結果和剛剛收到的 X_A, V_1 一起傳送給 S。

步驟五. S→A：Sid, V_3, V_4

S 收到資料後，解開 V_1, V_2，可以得到 A 和 B 的 ID，進一步取得 A 和 B 各自的密碼。接著從 $g^{(a \cdot pw_A)(pw_A)^{-1}}$ 取得 g^a，從 $g^{(b \cdot pw_B)(pw_B)^{-1}}$ 取得 g^b，計算出 $V_3 = E_{g^{az_1}}(M_1 = pw_A \oplus g^a, X_B, g^{ab})$ 和 $V_4 = E_{g^{bz_2}}(M_2 = pw_B \oplus g^b, X_A)$ 後傳出。

步驟六. A→B：Sid, V_4, V_5

A 收到資料後，將 V_3 解開，計算 $M_1 \oplus pw_A$ 的值是否等於 X_A，如果是，則算出 $V_5 = E_{g^{ab}}(ID_A, ID_B, g^a, g^b)$ 後，和 V_4 一起傳出。

B 收到 V_4, V_5 後，先解開 V_4，使用自己所擁有的密碼 pw_B 驗證是否合法，如果是，再解開 V_5 以檢查資料是否正確。最後的金鑰可以是 $K_{AB} = h(ID_A, ID_B, g^{ab})$。

三、效能及安全性分析

3.1 效能分析

表 3.1 和 3.2 在比較相關的機制之間所需要的回合數、使用隨機亂數的個數，以及指數運算、雜湊函數的使用次數。由這兩張表我們可以看出，我們採用了資料加密的方法，雖然多了額外的成本及回合數，但是相對的，我們減少了使用雜湊函數的成本。

表 3.1　2P-AEKE 的效能分析

	Lee-Lee[6]	YOON-YOO[3]	Our.
匿名	No	No	Yes
回合數	4	3	4
隨機亂數#	2	2	2
指數運算#	2+3 *	2+3	2+2
雜湊函數#	2+2	3+3	0+0
加/解密#	0+0	0+0	1+1

#：表示使用的次數。

*：表示 A+B 的次數。

表 3.2　經由第三方通訊的效能分析

	S-3PEKE [8]			Chung-Ku [4]			Chien [5]			Our.		
匿名	No			No			No			Yes		
回合	5			5			6			6		
	A	B	S	A	B	S	A	B	S	A	B	S
隨機亂數#	1	1	1	1	1	1	1	1	2	1	1	2

雜湊函數#	4	4	2	4	4	2	5	5	4	0	0	0
指數運算#	3	3	4	3	3	4	3	3	4	3	3	4
加/解密#	0	0	0	0	0	0	0	0	0	3	3	2

3.2 安全性分析

我們根據以下幾項常見的攻擊，來進行安全性的分析。

會議金鑰的安全性(Session key security)：會議金鑰的安全性指的是當協定城成功的執行時，只有正確的通訊方可以取得會議金鑰。而在我們的協定中，要確定金鑰是可以信任的，必須擁有挑戰的亂數 a 和 b，而它們分別的由 Diffie-Hellman 問題(DHP)和金鑰加密所保護著，所以所提出的協定提供了會議金鑰的安全性。

中間人攻擊(Man-in-middle attack)：在我們的協定中，使用了密碼來防止中間人攻擊，而密碼則由 Diffie-Hellman 問題保護著，非法的攻擊者無法取得密碼進行攻擊，所以可以抵擋中間人攻擊。

重送攻擊(Replay attack)：假設攻擊者攔截了傳輸中的資料，因為傳輸的資料都有經過加密處理，攻擊者無法藉由從上一次攔截到的資料來完成這次的認證，所以可以抵擋重送攻擊。

向前安全(Perfect forward secrecy)：向前安全指的是當我們假設在一段時間下來，密碼被破解了，但是之前所通訊的內容仍然是安全的。在我們的協定中，每回合的會議金鑰都是由不同的隨機變數所產生，隨機變數間都是獨立不相關的，因此，每次的會議金鑰也會是獨立的，而向前安全也因此成立。

離線的猜測攻擊(Off-line guessing attacks)：要成功的完成離線式的猜測攻擊，攻擊者必須經由公開的資料傳輸，來驗證他的猜測是否正確。在 2-party 的情境中，假設攻擊者偽裝成 A，那他可以取得由 B 回傳的資訊 Y，接著他對密碼進行猜測 pw^* 並找出偽造的 $M_1^* = g^a \oplus g^{pw^*}$，所以攻擊者又必須面對到 DHP，猜測攻擊無法成功。而在 3-party 的情境下，攻擊者一樣必須面對到 DHP 的問題，所以可以抵擋密碼猜測攻擊。

四、結論

匿名功能在很多的商務應用上已是迫切需求。在這篇文章中，我們針對 2-party 情境及 3-party 情境分別提出匿名式認證金鑰協定。相較於非匿名功能機制，我們的方法只些微增加一點計算量，因此仍是十分有效率的機制。

五、參考文獻

[1] C.L. Hsu, T.S. Wu, T.C. Wu, C. Mitchell, "Improvement of modified authenticated key agreement protocol", Applied Mathematics and Computation, 142 (2-3), 2003, pp. 305-308.

[2] D.H. Seo, P. Sweeney, "Simple authenticated key agreement algorithm", Electronics Letters, 35 (13), 1999, pp. 1073-1074.

[3] Eun-Jun YOON and Kee-Young YOO, "Improving the Lee-Lee's Password Based Authenticated Key Agreement Protocol", INFORMATICA, 2008 Vol. x, No. x, 1–14.

[4] H.R. Chung, and W.C. Ku, Three weaknesses in a simple three-party key exchange protocol, Information Sciences 178(1) (2008) 220-229.

[5] Hung-Yu Chien, "A Provably Secure Verifier-based Three-Party Key Exchange",

[6] K.J. Lee, B.J. Lee, "Cryptanalysis of the modified authenticated key agreement scheme", Applied Mathematics and Computation, 170 (1), 2005, pp. 280-284.

[7] N.Y. Lee, M.F. Lee, “Further improvement on the modified authenticated key agreement scheme”, Applied Mathematics and Computation, 157 (3), 2004, pp. 729-733.

[8] R. Lu, Z. Cao, Simple three-party key exchange protocol, Computers and Security 26 (2007) 94-97.

[9] W.C. Ku, S.D. Wang, “Cryptanalysis of modified authenticated key agreement protocol”, Electronics Letters, 36 (21), 2000, pp. 1770-1771.

[10] W. Diffie, M. Hellman, “New directions in cryptography”, IEEE Transaction on Information Theory, IT-22 (6), 1976, pp. 644-654.

[11] Y.M. Tseng, “Weakness in simple authenticated key agreement protocol”, Electronics Letters, 36 (1), 2000, pp. 48-49.